

7. **Imágenes fotográficas y grabaciones.** Se les prohíbe a los empleados tomar imágenes fotográficas, video u otras grabaciones en la propiedad de la empresa o en lugares en donde la empresa realiza actividades comerciales, mediante el uso de equipos que no sean los sistemas electrónicos y otros sistemas comerciales que la empresa mantenga o que sean propiedad de esta, sin el consentimiento expreso de la empresa. Los siguientes son algunos ejemplos de esta prohibición:

- tomar fotografías, digitales o de otro tipo, usando cámaras personales, teléfonos celulares u otros dispositivos en la propiedad de la empresa;
- grabar conversaciones en dispositivos de grabación tales como grabadoras, teléfonos celulares u otros dispositivos;
- grabar videos en videocámaras, teléfonos celulares u otros dispositivos.

La empresa se reserva el derecho de inspeccionar, observar, escuchar y obtener de parte del empleado todas las imágenes fotográficas, videos u otras grabaciones que haya realizado un empleado en la propiedad de la empresa o en un lugar en donde la misma realiza actividades comerciales o si la empresa sospecha razonablemente que las imágenes, los videos u otras grabaciones contienen información confidencial o sujeta a derecho de propiedad de la empresa o de una empresa con quien Stryker realiza actividades comerciales.

8. **Preguntas relacionadas con la política de los sistemas electrónicos y otros sistemas comerciales de Stryker.** Las preguntas relacionadas con esta política se deberán enviar al presidente, director de Recursos Humanos o director de Tecnología de la Información de la división, subsidiaria o unidad operativa correspondiente, al asesor general de Stryker o al vicepresidente de Recursos Humanos de Stryker.

9. **Infracciones de la política de la empresa.** Los empleados deberían informar al presidente, director de Recursos Humanos o director de Tecnología de la Información de su división, subsidiaria o unidad operativa, al asesor general de Stryker o al vicepresidente de Recursos Humanos de Stryker sobre cualquier infracción de la presente política. La infracción de esta política puede resultar en una medida disciplinaria, incluida la finalización de la relación laboral.

Joint Replacements

Trauma, Extremities & Deformities

Craniofacial

Spine

Biologics

Surgical Products

Neuro & ENT

Interventional Spine

Navigation

Endoscopy

Communications

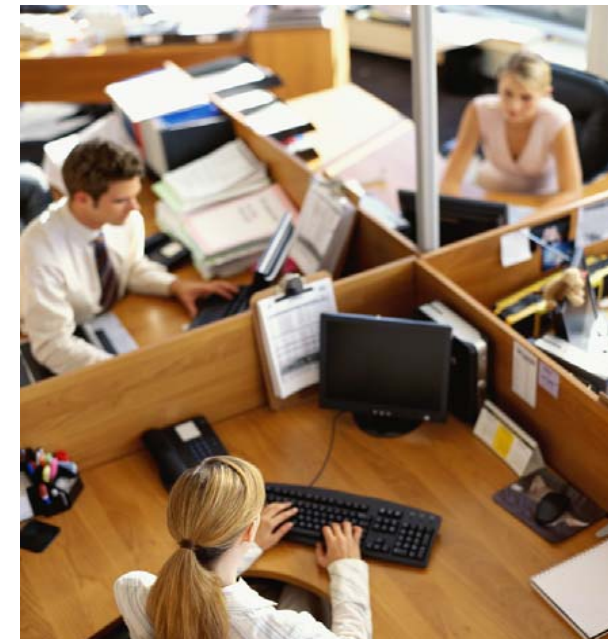
Imaging

Patient Care & Handling Equipment

EMS Equipment

Sistemas electrónicos y otros sistemas comerciales

Política empresarial número siete



**Copies of all Corporate Policies
may be found on
www.stryker.com/corporatepolicies**

2825 Airview Boulevard
Kalamazoo, MI 49002
t: 269 385 2600 f: 269 385 1062

Objetivo:

Establecer la política de la corporación Stryker sobre el uso de los sistemas electrónicos de Stryker y otros sistemas comerciales, los cuales incluyen, pero no limitados a, computadoras portátiles, de escritorio y de mano; correo electrónico; correo de voz; teléfonos; imágenes fotográficas (digitales y de otro tipo), asistentes digitales personales; dispositivos de grabación de videos; acceso a Internet, acceso a sistemas remotos e inalámbricos; conferencias de audio, video y web; máquinas de facsímiles; sistemas de registro horario electrónicos y credenciales de identificación asociadas; y otros servicios y equipos electrónicos o comerciales provistos por Stryker a sus empleados (denominados en el presente documento “sistemas electrónicos y otros sistemas comerciales”).

Alcance:

Esta política aplica para todos los empleados de Stryker pertenecientes a todas las ubicaciones de la empresa con el alcance permitido por las leyes vigentes. Si alguna disposición de la política no concuerda con las leyes locales que rigen para una determinada unidad de negocio de Stryker, esa unidad de negocio modificará la política a fin de que concuerde con las leyes locales y/o implementará una política aparte para que exista concordancia con dichas leyes locales, siempre que la política modificada se ajuste, con el mayor alcance posible, a los principios comprendidos en la presente política. Las disposiciones de esta política que concuerden con las leyes locales seguirán en vigencia.

Detalles:

1. Los sistemas electrónicos y otros sistemas comerciales son propiedad de la empresa. Stryker mantiene una variedad de sistemas electrónicos y otros sistemas comerciales. Estos sistemas se proporcionan a los empleados para ayudarlos en la realización de las actividades comerciales de la empresa. Todos los referidos sistemas y documentos, archivos, copias de seguridad, comunicaciones, imágenes y grabaciones que se creen, manejen o almacenen mediante estos sistemas son propiedad de Stryker y deben ser debidamente utilizados y protegidos contra el acceso no autorizado y la divulgación no deliberada.
2. Acceso por parte de la empresa. Stryker conserva el derecho a interceptar, acceder, controlar, revisar, copiar, modificar o eliminar de sus sistemas electrónicos y otros sistemas comerciales cualquier material generado o mantenido por los empleados de Stryker en cualquier momento y por cualquier motivo que la empresa considere adecuado, con o sin aviso previo al empleado. Dichos motivos pueden incluir, pero no están limitados a, la realización de las actividades comerciales de la empresa, el control de la calidad de

los servicios prestados por los empleados, garantizar el cumplimiento de las políticas de la empresa, garantizar la seguridad de los controles de la información personal de los empleados e investigar las acusaciones de conducta ilegal o incorrecta. El material cubierto por esta disposición incluye, pero no están limitados a, correo electrónico, correo de voz, imágenes fotográficas, conversaciones telefónicas, grabaciones de video y documentos, y archivos informáticos.

3. Acceso a correo electrónico, correo de voz y archivos informáticos por parte de los empleados de la empresa. Un empleado no debería acceder ni intentar acceder a las comunicaciones electrónicas, comunicaciones o mensajes de voz, o archivos informáticos de otro empleado sin la autorización de dicho empleado o del supervisor del mismo. Un empleado no debería compartir su contraseña o credenciales de inicio de sesión, salvo que así lo autoricen expresamente las políticas por escrito del Departamento de TI local; tampoco debería conservarlas en forma no protegida que permitiría el acceso de una persona no autorizada. Un empleado no debería intentar acceder, utilizar o alterar ninguna información personal o confidencial que se mantiene en el sistema de la empresa, salvo que cuente con una autorización comercial para hacerlo.
4. Divulgación de correo de voz o conversaciones grabadas. Se prohíbe a los empleados la divulgación del contenido de una conversación grabada en el sistema telefónico de la empresa, correo de voz y demás sistemas electrónicos y otros sistemas comerciales, sin el consentimiento expreso de la empresa.
5. Protección de la información confidencial y no pública. Los empleados que utilizan los sistemas electrónicos y otros sistemas comerciales tendrán el debido cuidado para proteger la información personal confidencial de los empleados y la información confidencial y no pública —ya sea que pertenezca a Stryker o que esté a su cargo—, del acceso no autorizado, la divulgación, la destrucción, la pérdida o la modificación.
6. Uso indebido de los sistemas electrónicos y otros sistemas comerciales. Además de cualquier requisito establecido por la división o el supervisor del empleado, los empleados tienen prohibido usar los sistemas electrónicos y otros sistemas comerciales de Stryker de las siguientes formas:
 - para establecer comunicaciones ofensivas, acosadoras, obscenas, despectivas o amenazantes;
 - para descargar, distribuir, visualizar, publicar, fotografiar, imprimir o enviar material pornográfico, obsceno, sexual, étnico, religioso, racial u otro tipo de material acosador, ofensivo o inadecuado;

- para instalar, descargar, distribuir o enviar programas, archivos o software de cualquier tipo; esto incluye, pero no limitado a, cartas en cadena, juegos, gusanos o virus informáticos de Internet u otras fuentes externas sin la autorización del Departamento de TI correspondiente;
- para instalar, descargar, distribuir, fotografiar o enviar material que infringiría cualquier ley de derecho de autor, marca comercial o patente;
- para conectar computadoras personales/del hogar con los sistemas informáticos de la empresa o manejar las actividades comerciales de la empresa en computadoras personales/del hogar o los correos electrónicos no pertenecientes a Stryker, sin la autorización del Departamento de TI correspondiente y del supervisor del empleado;
- para realizar promociones o promover las actividades de otros en nombre de cualquier organización externa;
- para realizar cualquier actividad comercial o con fines de lucro que no esté relacionada con las actividades comerciales de Stryker;
- para enviar cualquier publicidad de medios de comunicación, página de inicio de Internet, publicación de tableros electrónicos de noticias, mensaje de correo electrónico, imagen fotográfica, mensaje de correo de voz o cualquier otra representación o comunicación pública fuera de la empresa que pueda dañar la reputación de la empresa o la de sus socios comerciales;
- para actividades de caridad, salvo que estén autorizadas o patrocinadas por la empresa;
- para transferir cualquier información personal de empleados o información sujeta a derecho de propiedad no pública y/o información confidencial de Stryker o de una empresa con la que Stryker realiza actividades comerciales, sin la autorización previa de Stryker;
- para realizar cualquier contrato o acuerdo en nombre de Stryker sin la autorización previa de la empresa;
- para cualquier uso personal no razonable o cualquier uso que afecte o interfiera con las funciones laborales del empleado o de otros empleados;
- para cualquier fin ilegal o en violación del código de conducta de Stryker o cualquier política de la empresa.